UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/315,628	05/20/1999	BJORN MARKUS JAKOBSSON	15	6758

7590 06/22/2004

Joseph B. Ryan
Ryan, Mason & Lewis, LLP
90 FOREST AVENUE
LOCUST VALLEY, NY 11560

EXAMINER	
SIMITOSKI, MICHAEL J	

ART UNIT	PAPER NUMBER
2134	10

DATE MAILED: 06/22/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/315,628	JAKOBSSON, BJORN MARKUS	
	Examiner	Art Unit	
	Michael J Simitoski	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 April 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) ____ is/are allowed.

6)☒ Claim(s) *1-13,16,17 and 20-27* is/are rejected.

7)☐ Claim(s) *14,15 and 18-19* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *13 April 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

NORMAN M. WRIGHT
PRIMARY EXAMINER

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-27 are pending.

2. Applicant's remarks, dated April 13, 2004 has been received and considered.

Response to Arguments

3. Applicant's arguments, see paper #9 page 2, ¶4 – page 3, ¶1, filed April 19, 2004, with respect to the objection to the drawings have been fully considered and are persuasive. The objection of the drawings has been withdrawn.

4. Applicant's arguments filed April 19, 2004 have been fully considered but they are not persuasive.

Regarding the Menezes reference: On page 477, Menezes discloses a proof of a proof. The signature is already created. By concluding a disavowal, B is proving whether A has correctly proved the validity of the signature. In step 3, A is performing a proof. In step 8, B is proving the correctness of A's proof. Regarding the limitation "transmitting the proof information signal", as both A and B are performing steps of a proof (one proof to prove the signature's validity and the other to prove that the first verifier is not lying), proof information, as described in the claims is being transmitted. Therefore, the rejection of claims 1-2, 6, 11-12, 16, 22 & 25-27 are maintained.

Regarding applicant's argument against the Examiner's motivation, applicant has stated that the Examiner's "various" motivations to combine are unfounded in view of the references, with no specific argument to any of the motivations. The Examiner disagrees and the rejections are maintained and repeated below.

Regarding applicant's traversal of the Examiner's characterization (page 6 of applicant's remarks), the Examiner notes this traversal. However, the prior art does in fact teach the taking of an input of (g, y, m, s) for which $\log_g y = \log_m s$ described in the claims.

Regarding the inconsistencies noted by applicant, the Examiner apologizes for the oversight. This Office Action is made non-final to clarify any inconsistencies.

Claim Rejections - 35 USC § 101

5. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

6. Claims 1-10, 22-23, 25 & 27 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Regarding claims 1, 23 & 25, the claimed subject matter is a process that only manipulates abstract ideas or concepts. Nothing in the claim language suggests a dependence on a computer system, distinguishing the claimed method from a "pencil and paper" method. Claims 2-10 are rejected based on their dependence from claim 1.

Regarding claim 17, the claimed subject matter falls under two statutory classes as both an apparatus and method are claimed.

Regarding claims 22 & 27, the claimed subject matter is embodied on a computer-readable medium; however, the method steps claimed are directed to non-statutory subject matter and are directed to software *per se*.

To expedite a complete examination of the instant application, the claims rejected under 35 U.S.C. 101 (nonstatutory) above are further rejected as set forth below in anticipation of applicant amending these claims to place them within the four statutory categories of invention.

Claim Rejections - 35 USC § 112

7. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

8. Claim 17 recites the limitation "the method" in line 3. There is insufficient antecedent basis for this limitation in the claim.

9. Claim 17 rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The claim is indefinite because reference to "the method", line 3 does not further limit the apparatus claim 11.

Claim Rejections - 35 USC § 102

10. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

11. Claims 1-2, 6, 11-12, 16, 22 & 25-27 are rejected under 35 U.S.C. 102(b) as being anticipated by "Disavowal protocol for Chaum-van Antwerpen undeniable signature scheme" described in Handbook of Applied Cryptography by Menezes.

Regarding claims 1, 11, 22 & 25-27, Menezes discloses generating a signal/ w' and w (see page 477, steps 3 & 6) corresponding to information representative of first (see page 477, steps 1-7) and second (see page 477, step 8) proofs based on an operation associated with a cryptographic protocol (see page 476, Algorithm 11.122) wherein the first proof (see page 477, steps 1-7) is a proof that the operation/Algorithm 11.122 (see page 476) has been correctly performed, and the second proof (see page 477, step 8) is a proof that the first proof was correctly performed. The proof information signal/ w' and w is transmitted from the prover to the verifier (see page 477, steps 3 & 6) such that the verifier can determine if the operation associated with the cryptographic protocol is valid based on the proof information signal (see page 477, step 8).

Regarding claims 2 & 12, Menezes discloses a cryptographic protocol using an exponentiation operation (see page 477, step 2) and the proof information signal is based on a randomized instance of the exponentiation operation (see page 477, steps 2 & 3).

Regarding claims 6 & 16, Menezes discloses generating an indication that the prover is cheating if the second proof is not acceptable to the verifier (see page 477, step 8).

12. Claim 24 is rejected under 35 U.S.C. 102(e) as being anticipated by Mathematica: A System for Doing Mathematics by Computer, First Edition by Wolfram. Regarding claim 24, Wolfram discloses an apparatus/computer (page 3) operative/able to perform exponentiations

(page 15), logarithms (page 13) and comparisons (page 11). While Wolfram lacks disclosure of a processor, it is inherent that the computer described has a processor that performs the underlying mathematical calculations of the apparatus/computer.

Claim Rejections - 35 USC § 103

13. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

14. Claims 3 & 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Menezes, as applied to claims 1 & 11 above. Menezes, in describing the disavowal protocol, lacks disclosure of a blind proof. However, Menezes teaches that blind signature schemes prevent the signer from observing the message it signs (see page 475, § 11.8.1). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to make the Menezes signature, as described above, a blind signature to gain the benefit of preventing the signer from observing the message it signs. One of ordinary skill in the art would have been motivated to perform such a modification to prevent the signer from observing the message it signs, as taught by Menezes (see page 475, § 11.8.1).

15. Claims 10 & 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Menezes, as applied to claims 1 & 11 above, in view of "Distributed Provers with Applications to Undeniable Signatures" by Pedersen. Menezes, as described above, lacks the prover being a

distributed prover. However, Pedersen teaches that using a distributed prover allows verification by others if the signer is unable to perform required duties without the signer having to give away the secret (see page 228, § 5). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use a distributed prover to allow verification by others without the signer having to give away the secret. One of ordinary skill in the art would have been motivated to perform such a modification to allow verification by other than the signer without the signer having to give away the secret, as taught by Pedersen (see page 228, § 5).

16. Claim 21 is rejected under 35 U.S.C. 103(a) as being unpatentable over Menezes in view of Pedersen, as applied to claim 11 above, in further view of Computer Architecture: A Quantitative Approach, Second Edition by Patterson and Hennessey (Hennessey). Menezes, as described above, lacks the prover being a distributed prover. However, Pedersen teaches that using a distributed prover allows verification by others if the signer is unable to perform required duties without the signer having to give away the secret (see page 228, § 5). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use a distributed prover to allow verification by others without the signer having to give away the secret, as taught by Pedersen (see page 228, § 5). One of ordinary skill in the art would have been motivated to perform such a modification to allow verification by other than the signer without the signer having to give away the secret. Menezes, as modified, still lacks a distributed processor. However, Hennessey teaches that using multiple processors increases performance and improves availability (see p. 636) and are used in distributed, networked environments (see

p. 639). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to distribute processors amongst different machines to gain the benefits of increased performance and improved availability. One of ordinary skill in the art would have been motivated to perform such a modification to gain the benefits of increased performance and improved availability, as taught by Hennessey (see pp. 636-639).

Allowable Subject Matter

17. Claim 24 is allowed.

18. Claims 14, 15 & 17-19 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

19. The following is a statement of reasons for the indication of allowable subject matter:

Regarding claims 18 & 24, the prior art teaches taking an input of (g, y, m, s) for which $\log_g y = \log_m s$, however, the prior art relied upon fails to teach applying a key transformation protocol that produces a pair (G, Y) wherein G is a generator and Y is a public key, such that $X = \log_G Y$ can only be computed if $\log_g y = \log_m s$.

Regarding claims 14 & 15, the prior art relied upon fails to teach generating an indication that the operation was correctly performed if the first and second proofs are acceptable to the verifier. Further, the prior art relied upon fails to teach a step of generating an indication that the operation was not correctly performed if the first proof is not acceptable to the verifier but the second proof is acceptable to the verifier.

Regarding claim 17, the prior art relied upon fails to teach the steps set for in claims 7 & 17.

Regarding claim 19, the prior art relied upon fails to teach a key transformation protocol taking an input of the form (g, y, m, s, x) for which $\log_g y = \log_m s = x$ and generating a triple (G, Y, X) wherein X is a secret key, such that $Y = G^X$.

Conclusion

20. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. The Bellare reference is cited for teaching the verification of exponentiations.

b. The Chaum and Gennaro references are cited for teaching multiparty communication with threshold cryptography; threshold cryptography is applicable because when multiple parties are performing the computation, the need to prove that the exponentiations are done correctly increases.

21. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (703)305-8191. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m.. The examiner can also be reached on alternate Fridays from 6:45 a.m. – 3:15 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on (703)308-4789.

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks
Washington, DC 20231

Or faxed to:

(703)746-7239 (for formal communications intended for entry)

Or:

(703)746-7240 (for informal or draft communications, please label "PROPOSED" or "DRAFT")

Hand-delivered responses should be brought to Crystal Park II, 2121 Crystal Drive, Arlington, VA 22202, Fourth Floor (Receptionist).

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-9000.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MJS
May 28, 2004

NORMAN M. WRIGHT
PRIMARY EXAMINER